

# PRIVACY POLICY

Applied Marks is a brand owned by Griffith Hack.

GH PTM Pty Ltd trading as Applied Marks.

## 1. Contents

This Privacy Policy contains the following sections:

1. Contents
2. Overview
3. What Personal Information do we collect and hold?
4. How do we collect your Personal Information?
5. How do we use your Personal Information?
6. Who do we share your Personal Information with?
7. Keeping your Personal Information safe
8. Accessing, updating and correcting your Personal Information
9. How do you make a privacy complaint?
10. Contact details
11. **Appendix 1** – European Union General Data Protection Regulation

## 2. Overview

### a) The IPH Group

IPH Limited (ABN 49 169 015 838) is the holding company for a number of international intellectual property (IP) professional services firms operating under different brands (each an “IPH Service Firm”) and certain adjacent businesses. Certain IPH Service Firms also offer their services in some countries in collaboration with and with assistance by allied professional services firms with which they have exclusive contractual arrangements (each an “Alliance Firm”). The entities comprising the IPH Service Firms, Alliance Firms and the IPH adjacent businesses are in this Policy referred to together as members of the “IPH Group”.

GH PTM Pty Ltd and GH Law Pty Ltd (each company operating under the Griffith Hack brand in Australia) (“Griffith Hack”) and their related bodies corporate (as those terms are defined in Corporations Act 2001 (Cth)) are members of the IPH Group.

This Privacy Policy applies to Griffith Hack and all IPH Group members (collectively “we”, “us” or “our”).

This Privacy Policy explains how we collect, use, manage and disclose Personal Information, and how you can contact us if you have queries about our management of your Personal Information.

The Privacy Policy applies to all Personal Information submitted to or collected by us. By engaging us to provide professional services or submitting Personal Information to us, you accept the terms of this Privacy Policy, and consent to our use, collection, disclosure and retention of Personal Information as described in this Privacy Policy. If you do not agree to any provisions in this Privacy Policy, you should not disclose any Personal Information to us.

We reserve the right to modify this Privacy Policy at any time, so please review it frequently. Changes to this Privacy Policy will be published by posting an updated Privacy Policy on our website and are effective upon posting. Your continued use of our website, provision of instructions or information or receipt of our information or services, will signify your consent to be bound by this Privacy Policy.

You are welcome to print or download this Privacy Policy at any time. If you would like a hard copy of this Privacy Policy, or if you would like us to email or mail you a copy of this Privacy Policy, you can contact us and request a copy.

#### **b) Compliance with legal obligations**

We respect the privacy of all individuals who provide Personal Information to us. We operate in multiple jurisdictions, currently including Australia, New Zealand, Canada, Singapore, Malaysia, Indonesia, Thailand, Hong Kong, China and Philippines. The IPH Group members operating in those jurisdictions are bound by the respective privacy and personal data protection legislation in those jurisdictions. For such IPH Group members, where a requirement of any applicable legislation in the relevant country is inconsistent with this Privacy Policy, that legislative requirement will apply.

Any IPH Group member operating in a country is bound to comply with applicable privacy legislation in that country. For example, in Australia, this includes the Australian Privacy Act 1988 (Cth) and the Australian Privacy Principles set out in that Act; in New Zealand, this includes the New Zealand Privacy Act 2020 (NZ) and the information privacy principles set out in that Act; and in Canada, this includes the Personal Information Protection and Electronic Documents Act and all applicable provincial privacy laws. There are several references to these acts throughout this Privacy Policy.

To the extent any EU Personal Data (defined in Appendix 1) is collected, received, managed or processed by an IPH Group member, such IPH Group member will comply with the European Union General Data Protection Regulation 2016/279 in accordance

with Appendix 1 of this Privacy Policy. If this applies to you, it is important that you read Appendix 1 to ensure you are aware of how we will comply with our obligations and to review important consent requirements which are included in the Appendix.

### **3. What Personal Information do we collect and hold?**

“Personal Information” is information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, or about an individual who is reasonably identifiable.

In the course of our relationship with you, we are likely to collect a wide range of Personal Information about you. The type of Personal Information that we may collect will depend on our relationship with you, and the circumstances of collection. In general, the Personal Information we collect about you may include (but is not limited to):

- your first and last names;
- your date and place of birth;
- your phone number, facsimile number, residential address and email address;
- bank account details and credit / debit card details;
- any information or comments provided by you;
- any facts or opinions that are connected to an enquiry regarding your Personal Information that we are conducting on behalf of you or your organisation;
- reference details of you or your organisation related to the services we provide to you; and
- details about your use of our website through the use of cookies.

#### **a) Sensitive Information**

We do not generally collect “sensitive information” (such as information about ethnic origin, religious or political views, health information, tax file numbers etc.) in respect of website users, suppliers, business associates, clients and potential clients.

We only collect sensitive information reasonably necessary for one or more of the uses specified in section 5 of this Privacy Policy if:

- we have the consent of the individuals to whom the sensitive information relates; or
- the collection is necessary to lessen or prevent a serious threat to life, health or safety; or

- the information is required for another legal reason provided for under applicable privacy or other legislation.

## **b) Personal Information of Employees and Contractors**

In respect of current and potential employees, contractors and work experience persons, we may collect additional Personal Information including, but not limited to, personal resumes, third party references, bank details, superannuation details, tax file numbers, certain health information, emergency contact details and other employee or contractor records. We may also conduct criminal and other background checks on individuals who apply for a position with the IPH Group, commence employment or have a contracting arrangement with us. The results of such checks are held on our employee or contractor files for the duration of the employment, engagement or service, and may be retained after such relationship ceases, if required for legal, regulatory or business purposes.

## **4. How do we collect your Personal Information?**

### **a) Overview**

There are many ways in which we collect information from you.

We collect Personal Information directly from the individual concerned whenever reasonably practicable.

Sometimes, we collect Personal Information about you from a variety of other independent sources, including from publicly available sources (including social media), recruitment agencies, contractors, service providers and business partners. Where information is not obtained directly from the individual concerned, we obtain Personal Information in accordance with legal requirements.

The circumstances in which we may collect your Personal Information include, without limitation:

- when you have a face to face meeting with our staff and/or officers;
- when you attend our or third-party presentations, conferences or events;
- when you use our website or the website of a member of the IPH Group, including to request to receive a newsletter or other information from us;
- when you provide or offer to provide a product or service to us;
- when you obtain a product or service from us;
- when you communicate with us by e-mail, telephone or in writing;
- when you apply for employment or work experience with us or accept an offer of employment;

- when you enter into a contract with us;
- through share registries;
- from other members of the IPH Group (where permitted under this Policy);
- where you have consented to third parties sharing it with us, including our suppliers and providers of services and other business associates; and
- from publicly available sources, including newspapers and social media platforms such as LinkedIn, Facebook and Twitter.

**b) Providing third party Personal Information to us**

If, at any time, you provide us with Personal Information or other information about someone other than yourself, you warrant to us that you have that person's consent, including where applicable any necessary consent under section 6 of this Privacy Policy, to provide such information for the purpose specified and for us to treat such information in accordance with this Privacy Policy.

**c) Remaining Anonymous**

If, at any time, you provide us with Personal Information or other information about someone other than yourself, you warrant to us that you have that person's consent, including where applicable any necessary consent under section 6 of this Privacy Policy, to provide such information for the purpose specified and for us to treat such information in accordance with this Privacy Policy.

**d) Information about users of our websites and cookies**

Our Internet Service Providers record certain statistical information about users of our websites. This information is reviewed by us for statistical purposes and is not disclosed to third parties. We do not identify you or your browsing activities except, in the event of an investigation, where a law enforcement agency may exercise a warrant or other such power to inspect the internet service provider's server logs.

We use cookies on our websites to identify repeat viewers and make it easier for you to navigate our site. If you reject cookies, you may still use our site, but your ability to use some features of our site may be limited.

**5. How do we use your Personal Information?**

**a) General**

The primary purpose for which we collect, use and exchange your Personal Information is to establish your identity and to provide you with the products and services you have requested.

We may state a more specific purpose at the point we collect your information. If you do not provide us with the information that we request, we may not be able to provide you with our products or services.

In certain circumstances we may need to collect personal and sensitive information in order to comply with our legal obligations, such as anti-money laundering and counter-terrorism financing laws. If you do not provide us with the information we request, we will not be able to provide you with our products or services.

Our uses of Personal Information include but are not limited to:

- establishing your identity;
- communicating with you, including by email, mail or telephone;
- managing our relationship with you;
- advising you in relation to IP, legal and related matters;
- filing, prosecuting and maintaining applications for statutory protection of IP including patent, design, trade mark and domain name applications and registrations in Australia, New Zealand, Canada and overseas and engaging third parties to do so;
- conducting patent and trade mark opposition proceedings before the patent and trade mark offices and regulators in Australia, New Zealand, Canada and other jurisdictions;
- providing other professional services including advice with respect to litigation, dispute resolution services, appeals, commercial and regulatory legal advice, and IP watches and searches;
- providing you with updates, offers or proposals in relation to your matters and products and services that may be of interest to you;
- sending regular news alerts (and other correspondence) concerning developments in the field of IP and other areas that may be of interest to you;
- sending marketing and promotional material that we believe may interest you;
- for purposes necessary or incidental to the provision of goods and services to you;
- inviting you to events and functions;
- personalising and customising your experiences;
- managing and enhancing our products and services;
- investigating complaints made by you;

- in the case of employees and contractors:
  - to pay your wages, fees and employee & contractor entitlements;
  - conduct criminal checks and confirm your immigration status and right to work; and
  - to manage your relationship with us.

We may also use your Personal Information for purposes required or authorised by applicable laws or regulations, such as to prevent or investigate alleged crime or fraud. We may also use your Personal Information if it is necessary to prevent or lessen a serious threat to public health or public safety or if the use of the information is necessary for law enforcement or for the conduct of proceedings before any court or tribunal.

### **b) Marketing and Consent**

By supplying us with your Personal Information, you give us permission to disclose your Personal Information to members of the IPH Group and organisations that carry out functions (including marketing functions) on our behalf, or assist us to deliver our services, such as our business associates, contractors, agents or service providers, so that we can assess your likely needs, and contact you from time to time.

We may contact you to inform you about laws and developments in the field of IP and other products, services, events and resources we think would be of particular interest to you. We use tracking pixels in our communications to understand how recipients engage with our content (e.g., whether emails are opened or links are clicked). This helps us tailor and improve future communications. The permission you provide to us is not limited in time. You can, however, elect to opt out of receiving correspondence and other marketing materials from us by:

- contacting us using the contact information provided below in section 10 of this Privacy Policy; or
- by utilising an 'unsubscribe' facility on a communication we send to you.

If you opt out of receiving further communications from us, we will take steps to ensure you do not receive any such further information from us in future. Recipients of our news alerts and other correspondence may notify us at any time should they wish to discontinue receipt of emails and other communications from us.

### **c) Artificial Intelligence (AI) Tools**

We do not use any public-facing AI tools like chatbots to collect your Personal Information or interact with you. However, we may from time to time use your Personal Information in connection with AI-powered tools to support the delivery, improvement,

and personalisation of our services. This may include enhancing client experience, optimising service delivery, and developing more tailored solutions.

## **6. Who do we share your Personal Information with?**

Personal Information is disclosed and used by us to enable us to provide services to you and for the other purposes identified in section 5 above.

### **a) Members of the IPH Group**

We may receive and disclose Personal Information from or to other members of the IPH Group in accordance with this Privacy Policy, including entities located in various jurisdictions, including in Australia, New Zealand, Canada, Singapore, Malaysia, Indonesia, Thailand, Hong Kong, China and Philippines.

All disclosure of information by us within the IPH Group is subject to compliance with all legal requirements including but not limited to, for Australia and New Zealand, the *Code of Conduct for Trans-Tasman Patent and Trade Marks Attorneys 2018* issued by the Trans-Tasman Intellectual Property Advisory Board, other applicable legislation governing the conduct of our attorneys and professionals in other jurisdictions in which we conduct our businesses, and other IPH Group information sharing and conflicts of interest policies.

For the avoidance of doubt, whilst we may receive and disclose Personal Information from or to other members of the IPH Group, each IPH Service Firm (and where applicable its related Alliance Firm) maintains separate case management systems and no case related information is shared with another IPH Service Firm, except where such IPH Service Firm is formally engaged to provide professional IP services for the client, including as a foreign associate.

### **b) Disclosure and use of your Personal Information to and by third parties**

We may be required to disclose your Personal Information to certain third parties that may include:

- governmental offices (such as IP Australia, the Intellectual Property Office of New Zealand, the Canadian Intellectual Property Office, the Intellectual Property Office of Singapore and the IP offices of other jurisdictions);
- courts (such as the courts of Australia, New Zealand, Canada and other jurisdictions);
- government and law enforcement agencies and regulators;
- your agents, professional advisors, auditors or insurers;
- our financial, taxation or legal advisors;

- entities that assist us to deliver our services, including our business associates, contractors or service providers, including agents and associates in foreign countries;
- entities that assist or conduct mail outs on our behalf;
- debt collection companies;
- our clients (where information has been provided to us by someone other than our client);
- a purchaser or successor entity in connection with the sale of our business, a subsidiary of our business, or substantially all of its assets; and
- entities established to help identify illegal activities and prevent fraud.

As noted above, we may disclose your Personal Information to entities that assist us to deliver our services, such as our business associates, contractors, agents or service providers and, as noted elsewhere in this Privacy Policy, our Alliance Firms. These third parties may change from time to time. Some examples include technology and internet service providers, data storage providers, digital mail providers who send communications on our behalf and their implementation partners. We may also use graphic designers, printers and posting services to assist us with design, printing and distribution of communications. Where it is necessary for Personal Information to be provided to a third party in connection with the provision of a service to us, we will take reasonable steps within our power to prevent the unauthorised use or unauthorised disclosure of the Personal Information.

In relation to our disclosure of Personal Information to third parties such as agents and associates in foreign countries, we will make such disclosures when we are instructed to do so by our clients in relation to their matters in order to provide our services, or as may be required by law. You agree that, subject to any additional obligations under applicable laws, third parties who receive Personal Information from us may use and disclose the Personal Information subject to their respective privacy policies and laws applicable to them.

We do not disclose Personal Information to third parties for the purpose of third party direct marketing.

From time to time, we may provide third parties with information in the form of statistical representations about our users collectively and for the purpose of statistical analysis. Where we provide such information to third parties for this limited statistical purpose, we will not provide information in such a way that your identity may be obtained. To the extent this information does not constitute Personal Information (as defined in the Australian *Privacy Act 1988* (Cth), the *New Zealand Privacy Act 2020* (NZ) or the Canadian *Personal Information Protection and Electronic Documents Act* or

applicable provincial privacy legislation), or is otherwise not governed by applicable privacy legislation in the relevant jurisdiction, the Australian Privacy Principles, the New Zealand information privacy principles, the privacy principles set out in the National Standard Of Canada entitled “Model Code for the Protection of Personal Information” or other applicable privacy legislation, this Privacy Policy will not apply.

**c) Other permitted disclosures**

We may also disclose your Personal Information under the following circumstances:

- when you have consented to such disclosure;
- when you would reasonably expect us to use or disclose your Personal Information in a certain way;
- when authorised or required to do so by a court or under applicable laws or regulations (for example, a subpoena), or where requested by a government agency;
- where we consider a company or an individual may be engaged in fraudulent activity or other deceptive practices of which a governmental agency should be made aware;
- to appropriate persons, where your communication suggests possible harm to yourself or others; or
- when disclosure is reasonably necessary for a law enforcement related activity.

**d) Cross-border disclosure of your Personal Information**

We may disclose your Personal Information offshore for various reasons, such as for the purposes of:

- obtaining legal or other IP professional services in foreign countries;
- obtaining IP protection in foreign countries; or
- for administrative and other purposes within the IPH Group to facilitate the conduct of our businesses.

The types of foreign entities to which we may disclose your Personal Information include:

- members of the IPH Group located in various countries, including in Australia, New Zealand, Canada, Singapore, Malaysia, Indonesia, Thailand, Hong Kong, China and Philippines and any other jurisdictions in which we may operate in the future;

- our associates, agents or other legal or professional service provider firms in foreign countries;
- government bodies and other entities that administer IP in overseas jurisdictions; and
- our service providers located overseas, which may include technology and internet service providers, data storage providers and digital mail providers who send communications on our behalf.

You agree and acknowledge that the overseas recipients of your Personal Information will be subject to the privacy laws of their local jurisdiction. These overseas privacy laws are likely to be different to:

- if we are located within Australia, the Privacy Act 1988 (Cth) and the Australian Privacy Principles;
- if we are located within New Zealand, the Privacy Act 2020 (NZ) and information privacy principles set out in that Act;
- if we are located within Canada, the Personal Information Protection and Electronic Documents Act, the information privacy principles set out in that Act and applicable provincial privacy legislation; or
- in the other jurisdictions in which we operate, other applicable personal data protection legislation,

such that overseas recipients may not be required to protect your Personal Information in a way that provides comparable safeguards to those in your own jurisdiction and you may not be able to seek redress in the relevant overseas jurisdiction in relation to breaches of your privacy.

You acknowledge and agree to such international data and information transfers with respect to Personal Information of the nature described in this section 6.

For our Australian businesses, clause 8.1 of the Australian Privacy Principles contained in Schedule 1 of the *Privacy Act 1988* (Cth) provides that if we disclose Personal Information about an individual to a recipient based outside of Australia, then we must take such steps as are reasonable in the circumstances to ensure the overseas recipient does not breach the Australian Privacy Principles in relation to such information. An exception to this is if we obtain your consent. We intend to rely on this exception in the following way. Unless you notify us in writing to the contrary, you will be taken to have consented to the disclosure by our Australian businesses of Personal Information to overseas recipients on the basis that:

- clause 8.1 of the Australian Privacy Principles will not apply to such disclosure;

- the individual whose Personal Information is disclosed will not be able to seek redress under the *Privacy Act 1988* (Cth);
- the overseas recipient may not be subject to any privacy obligations or to any principles similar to the Australian Privacy Principles;
- the individual may not be able to seek redress in the overseas jurisdiction; and
- the overseas recipient is subject to a foreign law that could compel the disclosure of Personal Information to a third party, such as an overseas authority.

For our New Zealand businesses, information privacy principle 12 contained in section 22 of the *Privacy Act 2020* (NZ) provides that we may disclose Personal Information about an individual to a person or entity based outside New Zealand in certain instances if the individual authorises the disclosure to the overseas recipient after being expressly informed by us that the overseas recipient may not be required to protect the information in a way that, overall, provides comparable safeguards to those in the *Privacy Act 2020* (NZ). Given the express disclosures in this section 6(d) regarding overseas disclosures, unless you notify us in writing to the contrary, where applicable, you will be taken to have authorised the disclosure by our New Zealand businesses of Personal Information to overseas recipients.

Similar provisions may exist under privacy legislation in other jurisdictions in which members of the IPH Group are located. If such provisions are applicable to a member of the IPH Group holding your Personal Information, you acknowledge and consent to such cross-border disclosure on the basis outlined above (substituting references to the standards and remedies available under the applicable privacy legislation in the relevant entity's jurisdiction). Please note that privacy laws in other jurisdictions may provide for a different level of protection in respect of Personal Information than that which is applicable in your jurisdiction. If you would like to receive more information about our policies and procedures in relation to the cross-border disclosure of your Personal Information or our use of service providers in other jurisdictions, please contact our Privacy Officer at the address given below.

## **7. Keeping your Personal Information safe**

### **a) Security**

We make every effort to ensure Personal Information is kept secure and take reasonable steps to protect it from misuse, loss, interference, unauthorised access, modification or disclosure.

In terms of system security, here are some of the things we do to protect your Personal Information:

- we store Personal Information in a variety of formats including on databases, in hard copy files and on personal devices, including laptop computers;
- we retain Personal Information in secure hard copy and electronic files;
- we use firewalls, standard software protection programs, password access protections and secure servers;
- Personal Information in files that have been closed and archived may be stored in our offsite storage facility. We take reasonable steps to ensure that any third parties who handle files maintained in offsite facilities (including online data storage facilities) act consistently with this Privacy Policy;
- we regularly review our security arrangements to ensure we are taking reasonable and technically feasible steps available at the time to protect your Personal Information; and
- we take reasonable steps to destroy, erase or permanently de-identify Personal Information as soon as practicable if it is no longer required by us (including being required for record keeping or legal purposes) in accordance with the IPH Group Personal Information Data Retention and Destruction Policy.

As you will appreciate, since no system is 100% secure or error-free, we cannot guarantee that your Personal Information is totally protected, for example, from hackers, interference or misappropriation. You acknowledge that the security of online transactions and the security of communications sent by electronic means or by post cannot be guaranteed. You provide information to us via the internet or by post at your own risk. We cannot accept responsibility for misuse or loss of, or unauthorised access to, your Personal Information where the security of information is not within our control.

If you suspect any misuse or loss of, or unauthorised access to, your Personal Information, please contact us immediately using the contact details set out in section 10.

In the event of a data breach involving a loss of, unauthorised access to or misuse of your Personal Information, we will report such breach to you and any relevant authority as required by law.

#### **b) Third party websites**

Our website may contain links to other websites. You acknowledge that we are not responsible for the privacy or security practices of any third party (including third parties to whom we are permitted to disclose your Personal Information in accordance with this Privacy Policy or any applicable laws). The collection and use of your information by such third party/ies may be subject to separate privacy and security policies.

## **8. Accessing, updating and correcting your Personal Information**

We use reasonable endeavours to ensure that the Personal Information we collect, use and/or disclose is accurate, complete and up to date.

We request that you keep the information we hold about you as current as possible by advising us of any changes or inaccuracies to your Personal Information in the manner outlined below so that we may continue to improve our service to you.

### **a) Making a request to access, update or correct your Personal Information**

You may ask us for access to your Personal Information or request that your Personal Information be updated and/or corrected. You may also request that we destroy or erase your Personal Information, or you may contact us if you have any questions or complaints about, or if you wish to restrict or object to, how we collect, use, disclose, manage or store your Personal Information. You can contact us for any of these reasons by using the contact details set out in section 10 of this Privacy Policy.

We will respond to your request, where required by law, within one (1) calendar month from the date your request is received. We will inform you if this timeframe is not achievable and extend this timeframe as permitted by applicable law.

We may charge a fee to cover the costs of meeting your request if your request is unfounded or excessive.

Unless we are required or permitted by law to refuse to do so, we will, on request, provide you with details of the Personal Information we have collected about you or update, correct and amend your Personal Information in accordance with your request. Where we are also required by applicable law to provide further information about the use or disclosure of your Personal Information we will do so upon your request.

### **b) Exceptions**

If we do not agree to provide you with access to, or to amend or erase, your Personal Information as requested or otherwise meet your requests, we will notify you accordingly. Where appropriate, we will provide you with the reason(s) for our decision and the mechanisms available to complain about the refusal. If the rejection relates to a request to change your Personal Information, you may make a statement about the requested change and we will attach this to your record.

In some circumstances, and subject always to legal obligations to the contrary, we may not be in a position to grant access to your Personal Information or otherwise meet your requests with respect to your Personal Information, including when:

- your Personal Information is not retrievable;
- the request is frivolous or vexatious; or
- providing access or otherwise meeting your request:
  - is reasonably likely to pose a serious threat to the safety of an individual or the public;
  - is likely to impact unreasonably on the privacy of others;
  - would reveal information which relates to existing or anticipated legal proceedings between you and us, which information would not be accessible by the process of discovery in those proceedings;
  - would impact on any negotiations between you and us;
  - is unlawful (including being unlawful as directed by a court or tribunal order);
  - would likely impact on actions being taken in relation to alleged unlawful activities or misconduct relating to our functions and activities;
  - would be likely to impact on any enforcement related activities conducted by any enforcement bodies; or
  - would reveal evaluative information in connection with a commercially sensitive decision-making process.

## **9. How do you make a privacy complaint?**

If you have a problem or complaint, please let us know. We will respond to a complaint as soon as possible and within 10 working days to let you know who is responsible for managing your complaint. We will also try to resolve the complaint within 10 working days. When this is not possible, we will contact you within that time to let you know how long it will take to resolve the complaint.

If you believe that we have not adequately dealt with your complaint, you may complain to:

- where we are located in Australia, the Australian Information Commissioner (<https://www.oaic.gov.au/privacy/privacy-complaints/lodge-a-privacy-complaint-with-us>);

- where we are located in New Zealand, the New Zealand Privacy Commissioner (<https://www.privacy.org.nz/your-rights/making-a-complaint/>);
- where we are located in Canada, the Office of the Privacy Commissioner of Canada (<https://www.priv.gc.ca/>),

or refer to your local privacy authority.

## **10. Contact details**

If you would like to update or correct your Personal Information, seek access to Personal Information we hold about you, or if you have any questions or complaints about how we collect, use, disclose, manage or store your Personal Information, you can contact us at:

### **GRIFFITH HACK**

**Contact Person:** Privacy Officer

**Email:** [mail@griffithhack.com](mailto:mail@griffithhack.com)

**Address:** Level 10, 161 Collins Street, Melbourne VIC 3000, Australia

**Telephone:** +61 3 9243 8300

**Facsimile:** +61 3 9243 8333

OR

### **IPH LIMITED**

**Company:** IPH Limited ABN 49 169 015 838

**Contact Person:** Privacy Officer

**Postal Address:** Level 24 Tower 2, Darling Park, 201 Sussex Street, Sydney NSW 2000 Australia

**Telephone:** +61 2 9393 0301

**Facsimile:** +61 2 9261 5486

**Email:** [privacy@iphltd.com.au](mailto:privacy@iphltd.com.au)

This Privacy Policy was last updated on 10 September 2025.

11. Appendix 1 – European Union General Data Protection Regulation

## **1. Application**

This Appendix only applies to the collection and processing of “**EU Personal Data**”. “EU Personal Data” means any Personal Information of an individual who is located in the European Union (“**EU**”) (whether the individual is a citizen of an EU country or otherwise). This section will apply to you and the processing of your EU Personal Data if you are located in an EU country. This section does not apply with respect to your Personal Information if you are located outside of the EU, even though you may be a citizen of an EU country.

For the purposes of this Appendix, the term “**process**” has the meaning given to it under the GDPR and may include any operation or a series of operations performed on EU Personal Data, including collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

EU Personal Data that is collected by us may have been sourced directly from you, a third party (e.g. our European associates) or implied from your use of our services.

We process EU Personal Data in accordance with this Appendix and our Privacy Policy. To the extent of any inconsistencies between other sections of our Privacy Policy and this Appendix in relation to the processing of EU Personal Data, this Appendix prevails.

## **2. GDPR Principles**

Any EU Personal Data will be:

- processed lawfully, transparently and in a fair manner;
- collected only for the purposes identified in this Privacy Policy or any other agreed specified purposes and not further processed in a manner incompatible with those purposes;
- collected in an adequate and relevant manner and limited to what is necessary in relation to the purposes for which the EU Personal Data is processed;
- kept current and up to date in accordance with section 8 of this Privacy Policy;
- stored in a form which permits us to identify you, but only for the period necessary in relation to the relevant purposes identified in this Privacy Policy;
- stored and processed securely to protect EU Personal Data against unlawful or unauthorized access and accidental loss, damage or disclosure in accordance with section 7 of this Privacy Policy.

### 3. Lawful bases for processing

We will only collect and process EU Personal Data where we have lawful bases. This may include where:

- you have given consent;
- the processing of EU Personal Data is necessary for the performance of a contract with you (such as to deliver the services you have requested or that have been requested on your behalf); or
- the processing of EU Personal Data is necessary for the purposes of “legitimate interests” of the relevant IPH Group member, provided that such processing does not outweigh your rights or freedoms. Some “legitimate interests” are listed in sections 5 and 6 of this Privacy Policy.

Where we rely on your consent to process personal data, you have the right to withdraw, restrict or decline your consent at any time and where we rely on legitimate interests, you have the right to object. If you have any questions about the lawful bases upon which we collect and process EU Personal Data, please refer to section 8 of this Privacy Policy.

We do not use automatic decision making, such as profiling, to make a decision that may produce a legal effect concerning a data subject of EU Personal Data.

### 4. Rights of EU Personal Data subjects

In addition to other rights you may have as set out in this Privacy Policy, you may exercise the data protection rights set out below in relation to your EU Personal Data:

- **Access and Portability:** a request can be made by you for a copy of your EU Personal Data (and any other information relating to your EU Personal Data permitted under Article 15 of the GDPR) held by us, in accordance with section 8 of this Privacy Policy. In addition, you may request to be provided with such EU Personal Data in a structured, commonly used and machine-readable format (including for the purposes of transferring to another party).
- **Restrictions and Objections:** You may request that we limit our use of your EU Personal Data or processing by requesting that we no longer use your EU Personal Data or limit how we use your data, this may include where you believe it is not lawful for us to hold your EU Personal Data or instances where your EU Personal Data was provided for direct marketing purposes and now you no longer want us to contact you.

### 5. Our responsibilities as a “data controller” and “data processor”

We may act as the “data controller”, the “data processor” or in some instances both the data collector and data processor simultaneously in relation to EU Personal Data.

We will be a data controller where we determine the purposes and means of the processing of EU Personal Data alone or jointly with others. To the extent we are a data controller with respect to EU Personal Data, we:

- set out in this Privacy Policy how we collect Personal Information (including EU Personal Data), how it is stored, to whom such Personal Information is disclosed and how the EU Personal Data is otherwise processed;
- only appoint processors under agreements that the processor will comply with the GDPR;
- will maintain a record of processing activities which are under our responsibility (where required by GDPR);
- cooperate with relevant authorities which enforce the GDPR;
- implement appropriate technical and organisation security measures to protect EU Personal Data and report any data breaches to authorities and affected individuals as required by the GDPR in accordance with section 7 of this Privacy Policy.

If a third party discloses EU Personal Data to us for a specific purpose, we will be acting as a data processor in processing the EU Personal Data for that purpose. Where we act as a data processor, we will:

- only act on the controller’s documented instructions;
- impose confidentiality obligations on all personnel who process the EU Personal Data;
- not appoint sub-processors without the prior written consent of the controller;
- at the instruction of the controller, return or destroy the EU Personal Data in accordance with section 7 (but subject to section 8) of this Privacy Policy;
- where applicable, assist the controller in complying with the rights of the data subjects of the EU Personal Data;
- maintain and keep accurate records of processing activities (where required by GDPR); and
- implement appropriate technical and organisation security measures to protect EU Personal Data and report any data breaches to controller without undue delay.

## **6. Disclosure to third parties**

If we are required to disclose your EU Personal Data to third parties, including data processors or sub-processors, we will notify the third party that it has an obligation to handle any EU Personal Data in accordance with the GDPR.

In the event we are responsible for a transfer of EU Personal Data outside of the EU, such transfer will be for the necessary and lawful performance of our services, including the establishment, exercise or defence of an IP or legal right.

## **7. Express consent to transfer**

Further to section 6 of this Privacy Policy, by providing us with your EU Personal Data, you are consenting to the disclosure of your EU Personal Data to third parties outside of the EU. You also acknowledge that we are not required to ensure that those third parties comply with their obligations under the GDPR.

If you have any questions, comments or complaints about our handling of your EU Personal Data or wish to contact us regarding your EU Personal Data, please use the contact details set out in section 10 of this Privacy Policy. Your requests will be handled in accordance with section 8 of this Privacy Policy.